SPOTLIGHT:
DATA

Why dealers cannot ignore the threat of the GDPR

Breaching the GDPR data protection law coming into force in May could cost UK dealers up to £17.5m or 4% of global turnover. They need to get ready now

British motor retailers are unprepared for new data protection laws. In a recent poll for am-online.com, only a fifth of respondents said they were confident that their data processes were ready for the introduction in May 2018 of the General Data Protection Regulation (GDPR), which will replace the Data Protection Act 1998.

The new law grants the UK's regulator, the Information Commissioner's Office (ICO) the power to enforce fines of up to €20 million (£17.5m), or 4% of a company's global turnover for the worst breaches.

Fines of that size, not to mention potential reputational damage, mean the need to evaluate internal operations – including the marketing of MOTs or services, the sale of aftercare products or the promotion of deals on new vehicles – identify any areas at risk from data breaches, and implement the necessary systems to safeguard against them, has never been more important.

So how do the new rules work, what are their key features, and more importantly, how will they dictate the ways dealers handle customer data? Here, we look at the four main parts of GDPR – responsibility for customer data; remit of the legislation; enforcing a breach; and headline fines.

RESPONSIBILITY FOR CUSTOMER DATA

Who will be responsible for the customer's data under the new GDPR rules? Currently, under the EU Directive 95/46/EC, the data controller – in most cases the dealer – is solely accountable for all customer data.

However, the new legislation will stipulate that both the data controller and the data processor, often a third-party provider, will be liable for any breach. Organisations that process personal data will no longer be required to notify the ICO of their data processing activities, but instead keep an internal record.

"The data controller, i.e. the organisation responsible for processing personal data, is legally responsible," said an ICO spokesperson. "This is the case under both the existing Data Protection Act and the GDPR.

"Employees of a data controller are almost always not controllers in their own right – they don't have the ultimate control over how the data is processed. However, businesses have a responsibility to ensure that staff are adequately trained in data protection."

Dan Moore, director of IT consultancy PKF Cooper Parry, said dealers will also be required to appoint a data protection officer to oversee the handling of all their data and compliance. However, he added that under the new rules it is the business, and not the individual, which would be liable.

"It's the business that'll be fined by the ICO; individuals wouldn't be liable for a data breach (unless it was a criminal act)," he said. "It's the business and therefore the business owners who are responsible for making sure all staff are well trained and following process and the law."

This may take the form of a data protection policy to ensure that employees are aware of their duties regarding customer information.

Simon Upton, group commercial director of digital specialist GForces, a data processor, said that as the data owners, dealers will be responsible for ensuring they receive the appropriate consent from the customer to collect and use their data in the first place, in the form of a privacy notice. They will also need to make sure that their data processing is managed in a compliant manner, he said.

"The important part is making sure that you appoint

> YOU HAVE TO BE CLEAR AT POINT OF COLLECTION WHAT YOU ARE COLLECTING, WHY YOU ARE COLLECTING IT, AND FOR HOW LONG YOU WILL KEEP IT
>
> DAN MOORE, PKF COOPER PARRY

a data processor with the appropriate mechanisms to process the data in a compliant manner," said Upton.

"Then, from a liability perspective, the challenge for retailers is in ensuring that they are confident they have collected their customer records correctly and have received the appropriate approval to contact those customers from the start date for GDPR on May 25 next year.

"They should, however, already be doing this under the Data Protection Act. In terms of supplier due diligence, ISO27001-certified suppliers should give them confidence of this."

REMIT OF THE LEGISLATION

The next issue for dealers to tackle will be determining the breadth and scope of the new legislation's remit governing held data. Under the new laws, all data held by a dealer, whether it is that of a customer or their own staff, will be treated in the same way, said Moore.

Above all, however, he said dealers will need to be explicit about who is collecting and receiving the data (the dealer or the manufacturer) and how the data will be used, as well as how the data will be protected and continually assessed.

Any current or new arrangements entered into with third parties to process data on a dealer's behalf must be signed off in writing and include various provisions that guarantee the data processor's compliance with GDPR. They should also be checked and amended as appropriate.

Such agreements may also be necessary to document third-party arrangements if they are undertaking marketing on a dealer's behalf or where a cloud software provider holds data on their behalf.

"Under GDPR, you have to have a purpose to have the data and you have to have controls around it," said Moore.

"If you collect someone's data, you can't just pass it around freely, you have to be clear at point of collection what you are collecting, why you are collecting it, and for how long you will keep it.

"Consent has to be opt-in as well, no more pre-ticked boxes."

Peter Flynn, managing director of Three60 CRM, a data processor, added: "The same rules apply to personal data held on staff as that of customers. It should be under lock and key, securely password-protected and with restricted access – all the usual things you would expect with any data given to any company."

While all personal data will be covered by GDPR, the dealer's own business data, including that held by fleet departments and business managers, will not be subject to the same rules as that of a private individual, according to the ICO.

"Personal data is personal data, whether it relates to people inside or outside an organisation," said the spokesperson. "Customers or staff, it makes no difference – information that could identify a living individual is personal data and subject to the same laws.

"Information about corporate entities, i.e. not personally identifiable individuals, is not personal data and does not fall under the remit of the Data Protection Act or GDPR."

SPOTLIGHT:
DATA

SPONSOR'S COMMENT

By Allison Nau, managing director, Cox Automotive Data Solutions

Big data, data science, data privacy – you can scarcely read the news without hearing something about data. But what is data, and why is it important?

Data is information about something – for example, a person or a vehicle. As the world becomes more digitised, more and more data is collected and available – and with advancements in computing, it is now possible to quickly analyse large volumes of data.

But why is this important? Businesses that use data effectively, to inform decision-making and automate manual processes, are selling cars more quickly and more profitably than the competition.

So where does one start? The first step is to take one decision or process which needs improvement, such as which cars to stock, or what to do with vehicles that are not selling.

The next step is to determine what data would make that decision better or the process more efficient. Then it is time to acquire and analyse the data, and once analysed, to act on it. Gaining the full benefits of data may require changes to existing operational processes, but those organisations that make those changes are realising significant commercial benefit.

As part of the world's largest automotive service organisation, Cox Automotive Data Solutions combines data from across the entire vehicle lifecycle to improve decision-making and process efficiency. With expert brands including Manheim, Motors.co.uk, Modix, incadea, Xtime and NextGear Capital in our group, we transform data into actionable insight, helping our clients improve their business results through data-driven decision-making.

■ **For more information, please contact Cox Automotive by phone on 0333 444 0428, by email at hello@coxautodata.com, or by post at 2 Angel Mews, London, EC1V 1NY.**

COX AUTOMOTIVE™
DATA SOLUTIONS

ENFORCING A BREACH

Should the worst happen and a breach occurs, there will be a set process in place that dealers must follow. This will take the form of reporting the initial incident, through to a full investigation and, if required, the ICO taking enforcement action, said Martin Hinckley, director of data protection and privacy at Go DPO EU Compliance.

"The process starts with the initial breach being reported to the ICO within 72 hours, including details of what happened and the remedial action you have taken, and the regulator then determining whether a further investigation is warranted," he said.

"Any investigation will be led by a case officer, who will determine the level of infringement and damage caused, and the ICO also reserves the right to investigate further if any new information comes to light.

"Then the data controller will also have to issue a final data breach report to the ICO, who will then deliver a judgment. If enforcement is necessary, the ICO will issue a letter of intent that the data controller can challenge through the legal process."

Upton believes one of the biggest changes under GDPR will be the mandatory requirement to report a breach. He added that the ICO will be providing further guidance on this.

He said: "The other issue is that with potentially lots of companies self-reporting, the ICO could quite soon be inundated with phone calls. Then the ICO has to decide how to prioritise which one they investigate first.

"For the retailers' part... they need to make sure that their handling of data is well documented, so if there is a breach and the ICO needs to come in and investigate they can show they have done their due diligence and they have appropriate processes in place, including making sure all their staff are appropriately trained."

The ICO spokesperson added: "The form of any investigation will depend on the individual case. Factors such as the number of individuals affected, the nature of the personal data involved, the measures (if any) an organisation has taken before and after the breach to mitigate its likelihood or after-effects are just some of the issues which could be taken into account."

> IT'S SCAREMONGERING TO SUGGEST THAT... MAXIMUM FINES WILL BECOME THE NORM. WE HAVE ALWAYS PREFERRED THE CARROT TO THE STICK
>
> ELIZABETH DENHAM, ICO

HEADLINE FINES

The consequences of a data breach for a business can be severe. The current maximum fine is £500,000, but that will be increased to 4% of a company's global turnover or £17.5m, according to the ICO.

Possibly more seriously, the ICO will also have the power to remove a dealer's right to handle customer data, which would almost certainly mean they would be forced to cease trading, given their reliance on it to promote products and services.

The ICO has made it clear that it will have a range of regulatory powers available for dealing with offenders. However, it also emphasised that fines would normally be a last resort, reserved for the worst data protection breaches.

Elizabeth Denham, the Information Commissioner, said: "It's true we'll have the power to impose fines much bigger than the £500,000 limit the Data Protection Act allows us. It's also true that companies are fearful of the maximum £17m or 4% of turnover allowed under the new law.

"But it's scaremongering to suggest that we'll be making early examples of organisations for minor infringements or that maximum fines will become the norm. The ICO's commitment to guiding, advising, and educating organisations about how to comply with the law will not change under the GDPR.

"We have always preferred the carrot to the stick."

Among the worst offences that would qualify for the stiffest penalty would be those that lead to discrimination of a data subject, identity theft, and a child's personal data being compromised, in addition to the marketing of sales and aftersales programmes without the customer's explicit consent, said Moore.

However, he added that in order to attract the highest penalty, the business would have had to have been completely negligent in the first place.

"To get the maximum fine, I'd expect a business to have been pretty much doing nothing to protect the personal information they had been keeping and then lost and it to be a big breach," said Moore.

"Something along the lines of saving everyone's bank details onto a website with a simple password as protection.

"If they'd taken steps such as encryption and removing sensitive details, but still got hacked the ICO would probably be more lenient."

Upton added: "The ICO has been quite clear that fines should be issued as a last resort. What is more harmful is the reputational damage to a business as a result of the breach, as this is not something which you can insure yourself against."

CONCLUSION

Data privacy and protection are sensitive issues and should be dealt with accordingly by dealers.

Before GDPR comes into effect next May, dealers need to take a host of new requirements, such as data ownership, into consideration, as well as implementing procedures to ensure they are fully compliant and don't fall foul of the potential penalties. ALEX WRIGHT